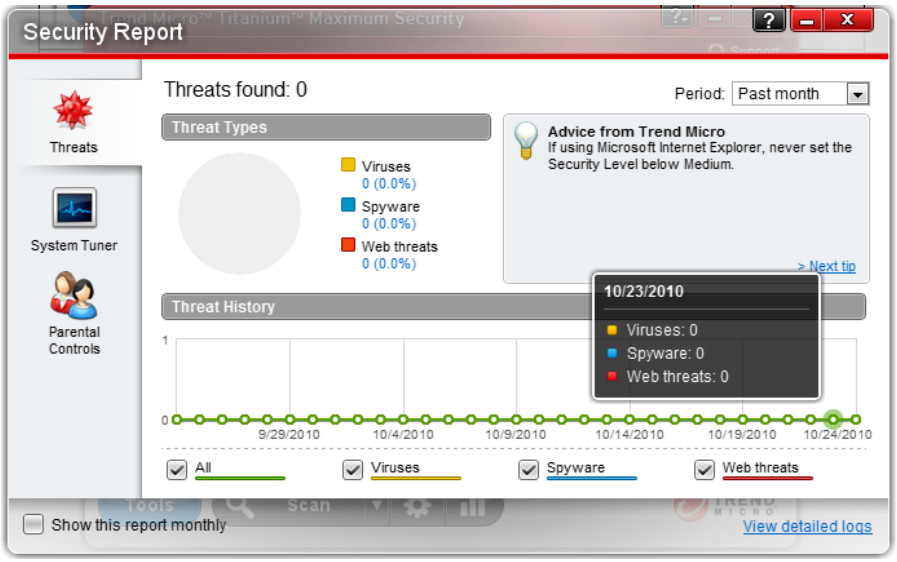
Trend Micro Titanium Maximum Security
User Manual

1. Main Panel

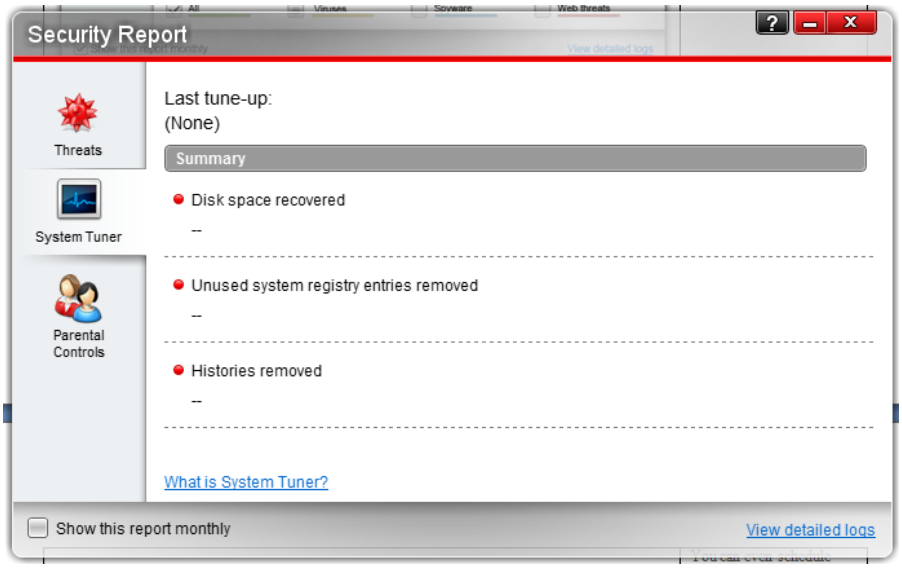
In the main panel by a large icon and the bar has been protective level of your computer, and below it there are three main areas of security and status indicator on your license.
Security Summary: when use this menu there is appearing new window which is showing
Security Report
Parental Controls:
System Tuner:
Subscription:

2. Security Report



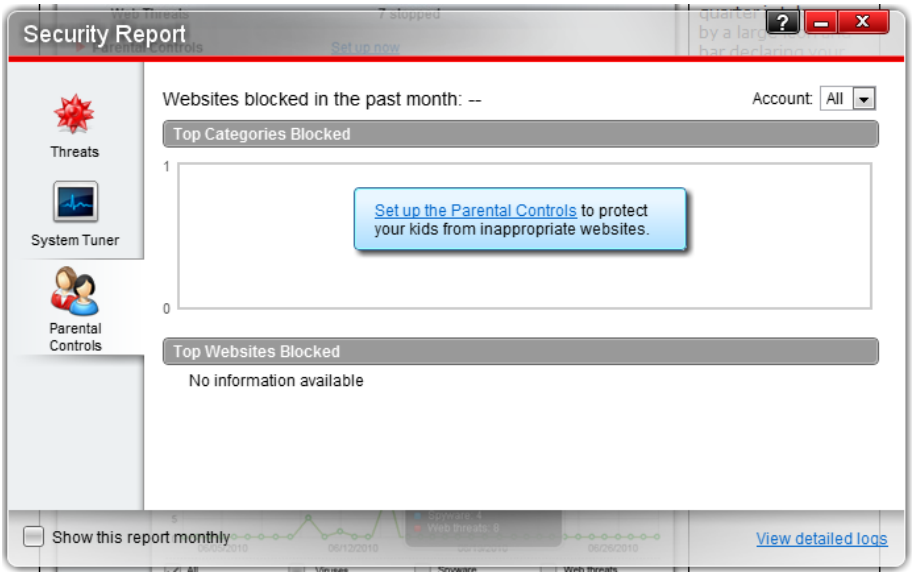
In Security Reports can see detailed reports with a graphical interface for number of viruses, spyware and web threats over time.
By selecting View detailed logs can be seen reports for all zaprahi zarpredeleni stopped by category:
Last Scan
Viruses
Spyware
Browser Cookies
Web Threats
Data Thief Prevention
Updates
Secure Erase
WIFI Advisor
System Tuner
Parental Controls
Network
Unauthorized Change Prevention
These logs can be exported and saved with button export

3. System tuner



System Tuner service can help you recover disk space, can make the launch of Microsoft ® Windows ® more quickly to clear your stories of instant messaging programs and to optimize the performance of your computer. You can even adjust automatically improve the performance of your computer and make his work more smooth and seamless.
More of that data link:
What is System Tuner?

4. Parental Control



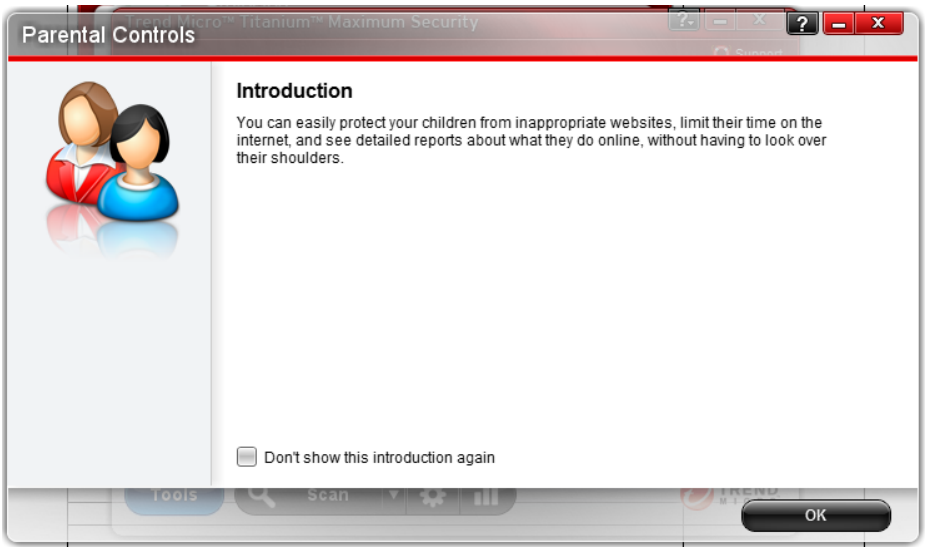
Parental Control gives you ability to determine how people use the Internet from this computer. You can prevent certain categories of sites to be opened, may be limited Internet access for a number of visits per day. You can also create rules that apply only for a person who enters this computer.
Detailed description of settings and vazmovnostite below

5. Tools

Form **Tools button** in main screen you can access:

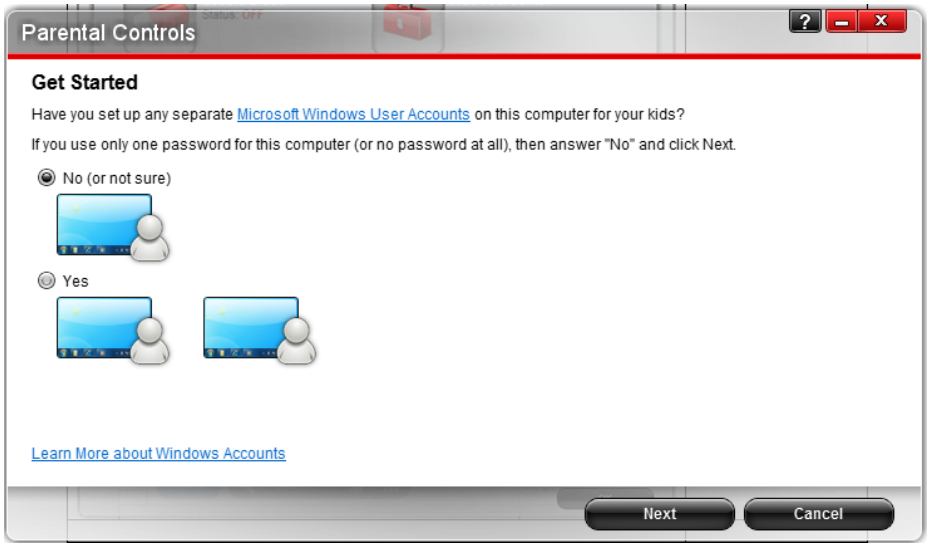
Parental Controls
System Tuner
Secure Erase
Data Thief Prevention
Trend Micro Vault
Free Tool Center

6.Parental Control


Parental Controls
Introduction
You can easily protect your children from inappropriate websites, limit their time on the internet, and see detailed reports about what they do online, without having to look over their shoulders.
Don't show this introduction again
OK

You can choose **Parental Controls** from main screen ot after press **Tools** button, then you can access Introduction screed for setting up feature for **Parental controls**

7. Parental Control

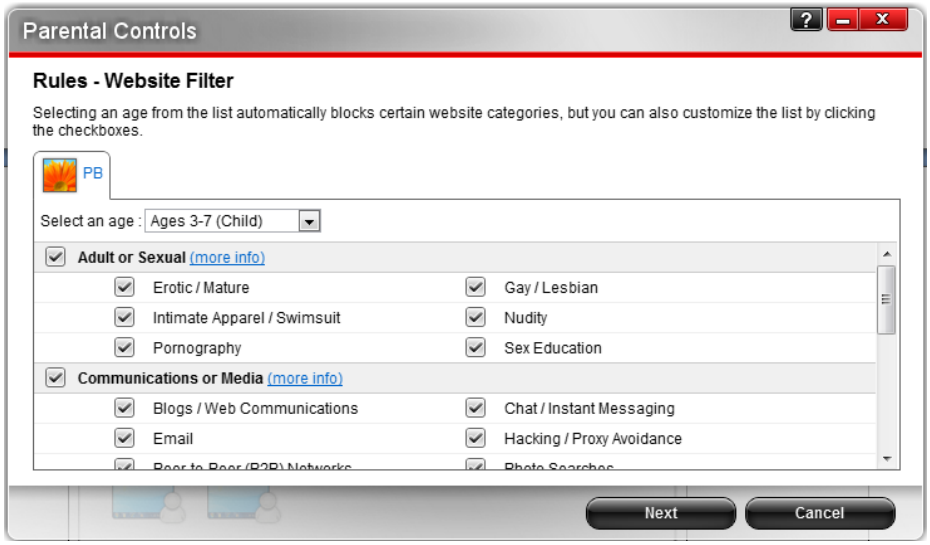

Parental Controls
Get Started
Have you set up any separate Microsoft Windows User Accounts on this computer for your kids?
If you use only one password for this computer (or no password at all), then answer "No" and click Next.
No (or not sure)
Yes
Learn More about Windows Accounts
Next
Cancel

Getting Started

The first time you try to use the Parental Controls, you will be asked if you have set any separate Microsoft Windows User Accounts on the computer. By setting up separate accounts for your kids, you can configure different rules for them by linking each Windows User Accounts to the Parental Controls. Otherwise, the same rules will apply to everyone using the computer.

Whether or not you have set up separate user accounts, the Parental Controls will then walk you through the process of setting up the rules for this protection.

8. Parental Control - settings



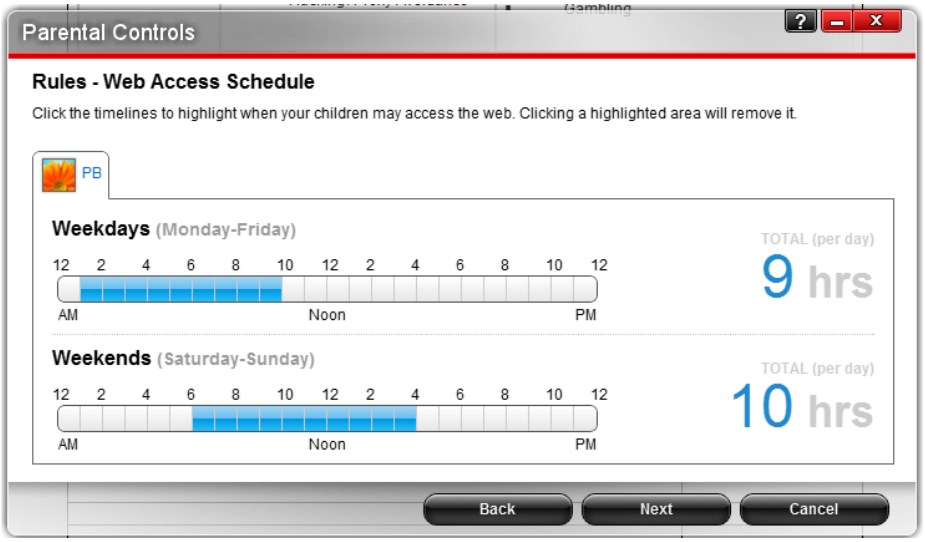
Website Filter

The Parental Controls let you filter different categories of websites based on three age groups: 3-7 (Child), 8-12 (Pre-teen), and 13-17 (Teen). The list below shows which specific categories are blocked by default for each age group.

9. Parental Control - settings

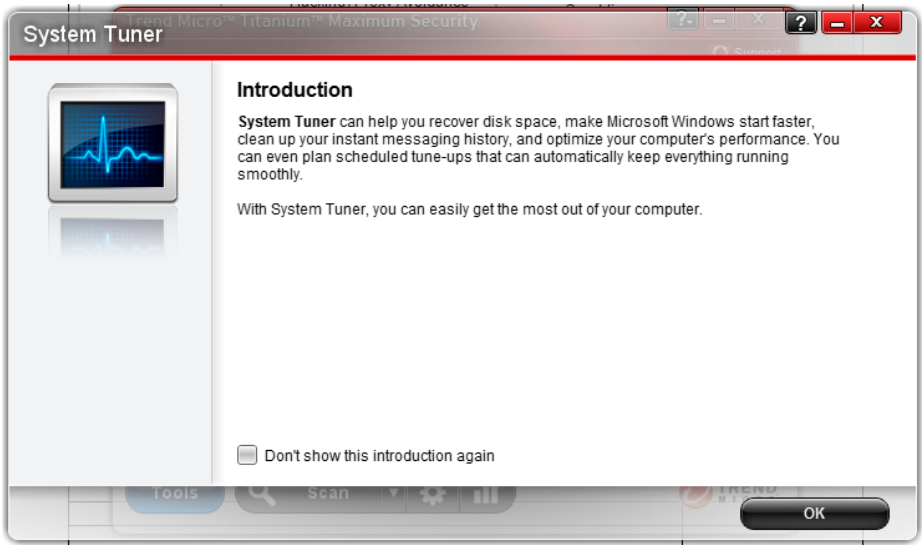
Age Group	Categories Blocked	
Ages 3-7 (Child)	All categories are blocked by default for young children.	
Ages 8-12 (Pre-teen)	**Adult or Sexual** ▪ Erotic / Mature ▪ Gay / Lesbian ▪ Intimate Apparel / Swimsuit ▪ Nudity ▪ Pornography ▪ Sex Education	**Controversial** ▪ Abortion ▪ Criminal / Questionable ▪ Cult / Occult ▪ Illegal Drugs ▪ Violence / Hate / Racism ▪ Weapons / Military
	Communications or Media ▪ Hacking / Proxy Avoidance ▪ Personals / Dating ▪ Social Networking	**Shopping and Entertainment** ▪ Alcohol / Tobacco ▪ Auctions ▪ Gambling
Ages 13-17 (Teen)	**Adult or Sexual** ▪ Erotic / Mature ▪ Nudity ▪ Pornography	**Controversial** ▪ Criminal / Questionable ▪ Illegal Drugs ▪ Violence / Hate / Racism
	Communications or Media ▪ Hacking / Proxy Avoidance	**Shopping and Entertainment** ▪ Alcohol / Tobacco ▪ Gambling
You can add or remove categories for any age group just by clicking the checkboxes next to any category on the list.		

10. Parental Control - settings


Parental Controls
Rules - Web Access Schedule
Click the timelines to highlight when your children may access the web. Clicking a highlighted area will remove it.
PB
Weekdays (Monday-Friday)
12 2 4 6 8 10 12 2 4 6 8 10 12
AM Noon PM
TOTAL (per day)
9 hrs
Weekends (Saturday-Sunday)
12 2 4 6 8 10 12 2 4 6 8 10 12
AM Noon PM
TOTAL (per day)
10 hrs
Back
Next
Cancel

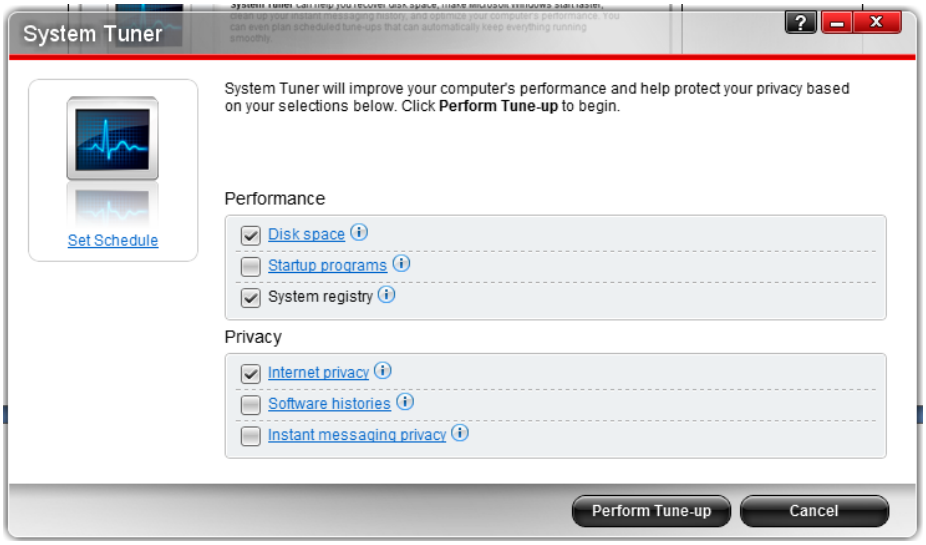
You can setup time interval when to be valid written rule and restriction for access.

11. Parental Control - settings


System Tuner
Introduction
System Tuner can help you recover disk space, make Microsoft Windows start faster, clean up your instant messaging history, and optimize your computer's performance. You can even plan scheduled tune-ups that can automatically keep everything running smoothly.
With System Tuner, you can easily get the most out of your computer.
Don't show this introduction again
OK

System Tuner optimizes your computer's performance and helps protect your privacy on the Internet. Before making any changes, System Tuner also backs up your system settings.

12. Parental Control - settings



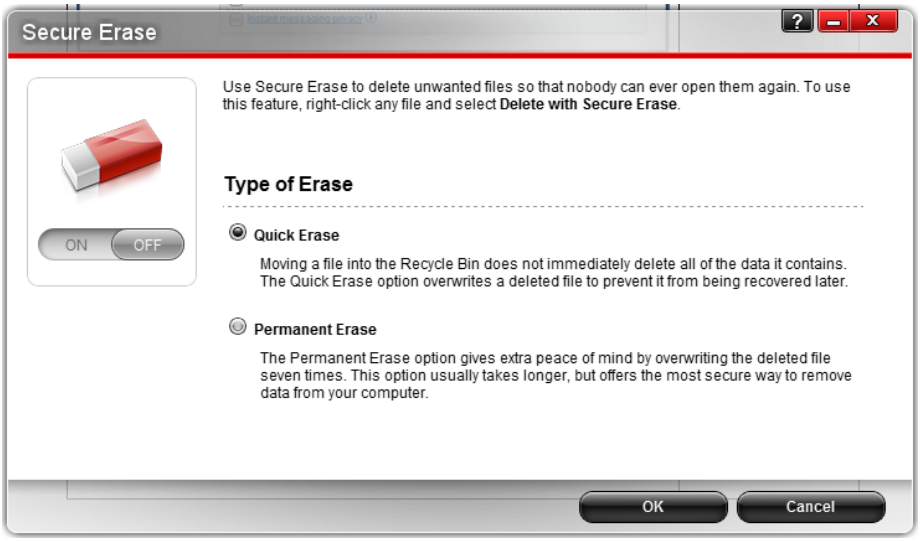
What benefits does System Tuner provide?
System Tuner can offer the following enhancements to your computer:

- **Disk space** — System Tuner checks for recoverable disk space in temporary folders, the Recycle Bin, and other locations. You can use the space recovered to store more programs and files.
- **Startup programs** — Most computers have several programs and services that start automatically when Windows™ opens. Many of these programs and services, including security software, must remain in memory for your benefit. However, computers with limited memory that run too many programs can slow down or become unresponsive. System Tuner can automatically find and delete autostart settings pointing at missing files to help prevent startup problems. If you thoroughly understand how Windows works, you can also choose to remove other autostart settings.
- **System registry** — The system registry contains all of your Windows and program settings. Unused, broken, or invalid entries cluttering the registry can affect your computer's stability and performance. Sometimes they can even prevent you from installing applications or starting Windows™. System Tuner can find and remove unneeded registry entries.
- **Internet privacy** — Websites use small text files called cookies to provide you with customized content or services. Your browser history lets you easily revisit websites. However, someone could also use this information to identify your computer and analyze what you view on the Internet. To help protect your privacy, System Tuner can delete cookies and browser history entries.
- **Software histories** — To help prevent spyware from gathering information about your computer, System Tuner can delete lists of files recently opened by Windows, Microsoft® Office software, media players, Windows search, and other programs. It can also delete the lists of files or programs recently opened from the Windows Start

button menu.

- **Instant messaging privacy** — To help maintain your privacy online, System Tuner can remove chat histories, recent screen names, lists of files downloaded, transaction logs, and other information generated by using Windows Live (MSN) Messenger, AOL Instant Messenger (AIM), and Yahoo! Messenger.

13. Secure Erase


Secure Erase
Use Secure Erase to delete unwanted files so that nobody can ever open them again. To use this feature, right-click any file and select Delete with Secure Erase.
ON
OFF
Type of Erase
Quick Erase
Moving a file into the Recycle Bin does not immediately delete all of the data it contains. The Quick Erase option overwrites a deleted file to prevent it from being recovered later.
Permanent Erase
The Permanent Erase option gives extra peace of mind by overwriting the deleted file seven times. This option usually takes longer, but offers the most secure way to remove data from your computer.
OK
Cancel

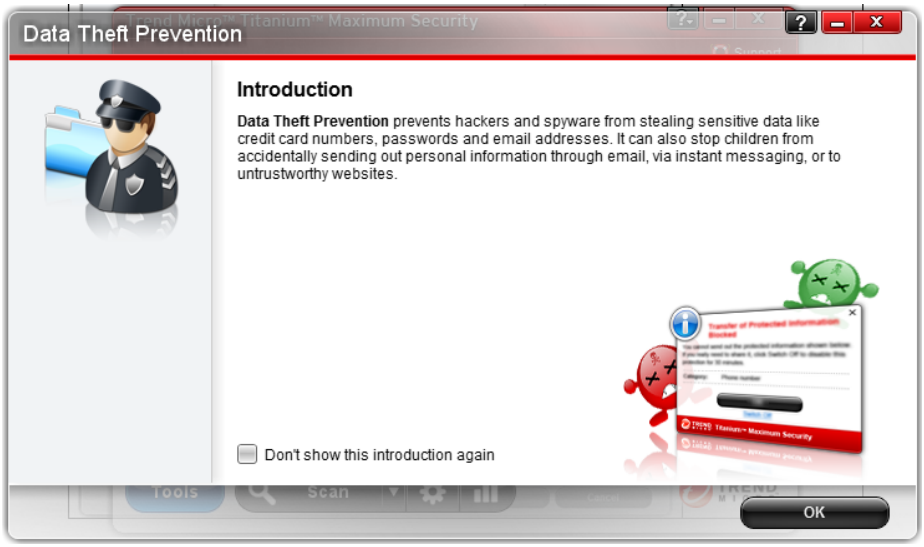
When you delete a file, Microsoft Windows just removes the directory information used to find it. The actual data still remains on your hard drive, and potentially available to someone with recovery tools.
After switching on this feature, mark the radio button to indicate what level of security you want from Secure Erase.

- **Quick Erase** will overwrite your unwanted files with random data, so that nobody can easily open them again.

- **Permanent Erase** can overwrite files with random data seven times for extra peace of mind, and meets United States Federal Government standards for data security.

You can then take advantage of this feature by right-clicking any file and selecting the **Delete with Secure Erase** option.

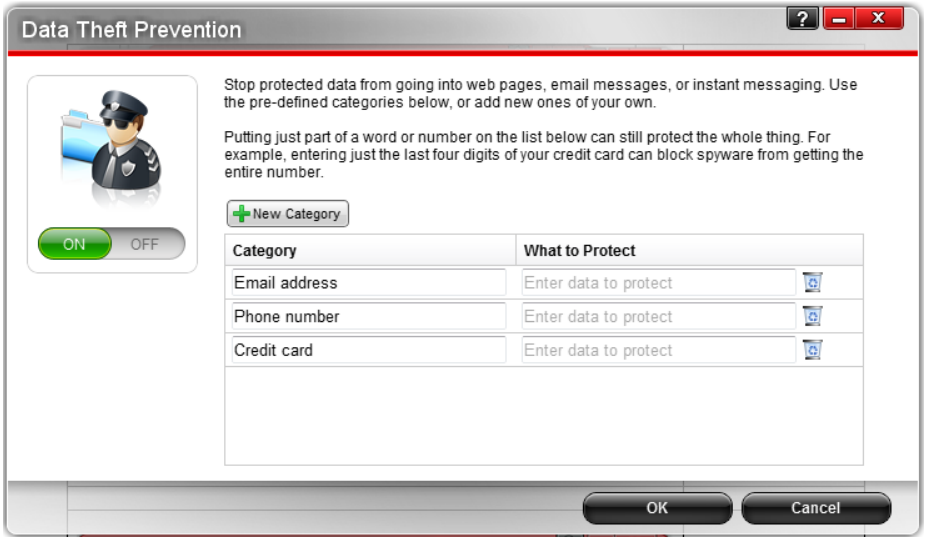
14. Data Theft Prevention


Data Theft Prevention
Introduction
Data Theft Prevention prevents hackers and spyware from stealing sensitive data like credit card numbers, passwords and email addresses. It can also stop children from accidentally sending out personal information through email, via instant messaging, or to untrustworthy websites.
Don't show this introduction again
OK

Data Theft Prevention

- Prevents theft of credit card numbers, passwords, email addresses and other sensitive data from hackers and spyware.

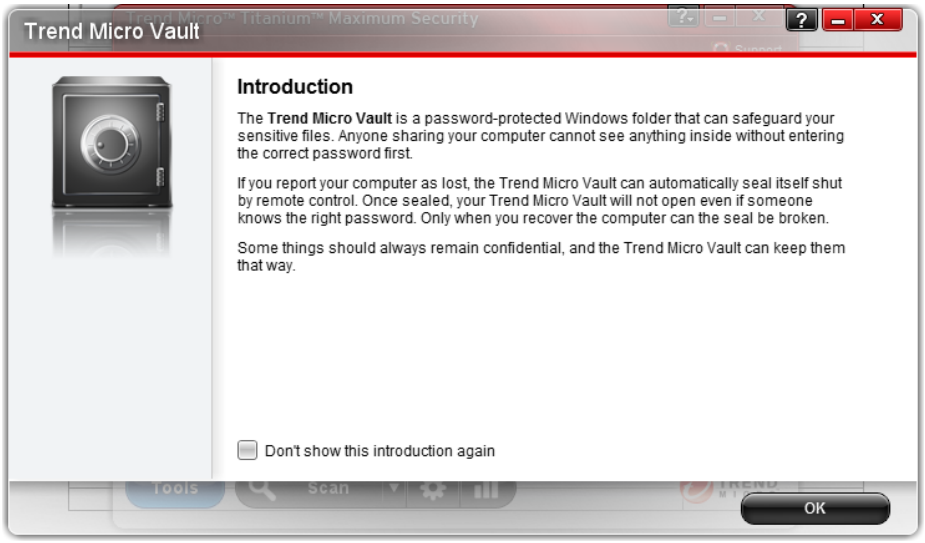
15. Data Theft Prevention - settings


Data Theft Prevention
Stop protected data from going into web pages, email messages, or instant messaging. Use the pre-defined categories below, or add new ones of your own.
Putting just part of a word or number on the list below can still protect the whole thing. For example, entering just the last four digits of your credit card can block spyware from getting the entire number.
New Category
ON
OFF
Category
What to Protect
Email address
Enter data to protect
Phone number
Enter data to protect
Credit card
Enter data to protect
OK
Cancel

This tool can protect sensitive personal information, such as credit card numbers or passwords for online services. Upon detecting any attempt to send protected information to the Internet, whether to a web page, by email or through an instant message, the transmission can be blocked automatically.

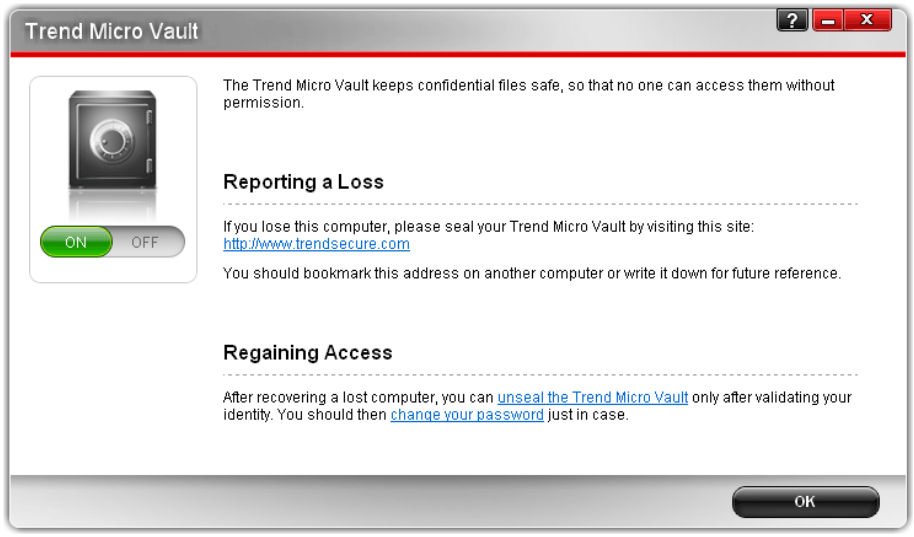
Data Theft Prevention monitors HTTP traffic (ports 80, 81, 8080, and any proxy server port you configure in your Microsoft® Internet Explorer® settings), but not HTTPS traffic (encrypted information cannot be filtered).

16. Trend Micro Vault – file protection


Trend Micro Vault
Introduction
The Trend Micro Vault is a password-protected Windows folder that can safeguard your sensitive files. Anyone sharing your computer cannot see anything inside without entering the correct password first.
If you report your computer as lost, the Trend Micro Vault can automatically seal itself shut by remote control. Once sealed, your Trend Micro Vault will not open even if someone knows the right password. Only when you recover the computer can the seal be broken.
Some things should always remain confidential, and the Trend Micro Vault can keep them that way.
Don't show this introduction again
OK

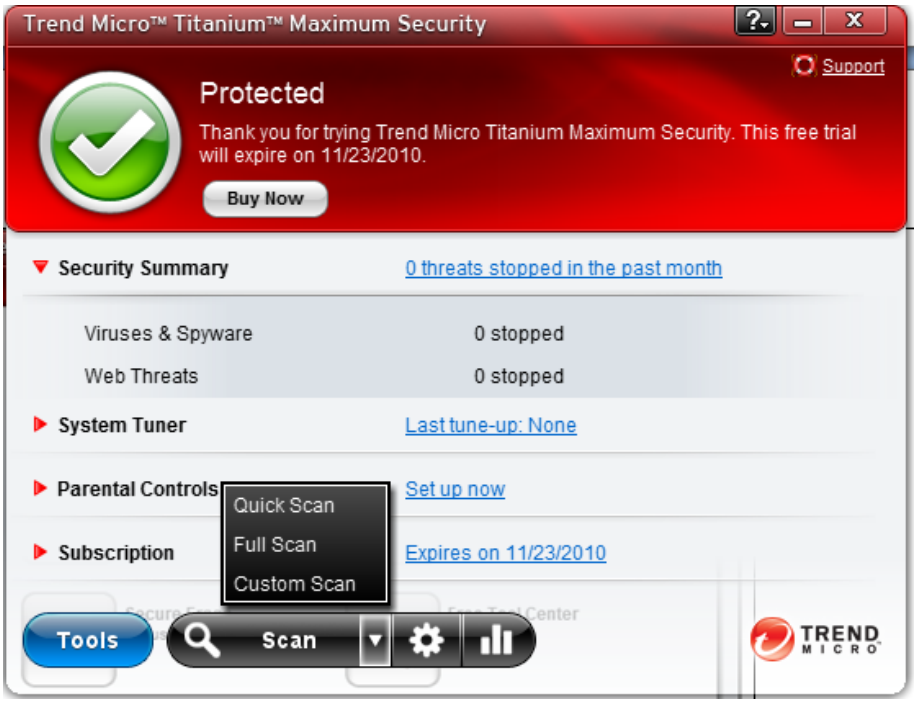
The Trend Micro Vault helps keep your sensitive files secure. You can easily block casual access to files in the vault, or seal the vault completely if your computer is lost or stolen.

17. Trend Micro Vault – file protection


Trend Micro Vault
The Trend Micro Vault keeps confidential files safe, so that no one can access them without permission.
ON
OFF
Reporting a Loss
If you lose this computer, please seal your Trend Micro Vault by visiting this site:
http://www.trendsecure.com
You should bookmark this address on another computer or write it down for future reference.
Regaining Access
After recovering a lost computer, you can unseal the Trend Micro Vault only after validating your identity. You should then change your password just in case.
OK

The Trend Micro Vault requires a password to open files inside. It regularly checks online to find out if you have reported the computer as lost or stolen. If that happens, the Trend Micro Vault automatically seals shut, blocking access to everything inside, even if someone has the correct password.

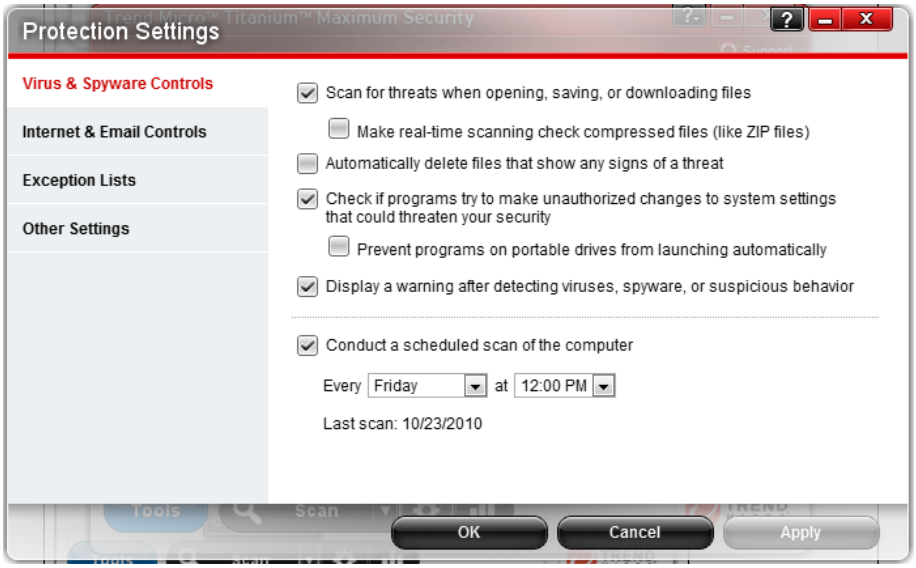
18. Main Panel - scanning



You can choose from three types of scans::

- **Quick Scan**
  Scans only the places where threats commonly hide
- **Full Scan**
  Scans the entire computer, including any external drives, except network drives
- **Custom Scan**
  Scans everything in the folders that you select

19. Protection settings


Protection Settings
Virus & Spyware Controls
Internet & Email Controls
Exception Lists
Other Settings
Scan for threats when opening, saving, or downloading files
Make real-time scanning check compressed files (like ZIP files)
Automatically delete files that show any signs of a threat
Check if programs try to make unauthorized changes to system settings that could threaten your security
Prevent programs on portable drives from launching automatically
Display a warning after detecting viruses, spyware, or suspicious behavior
Conduct a scheduled scan of the computer
Every Friday at 12:00 PM
Last scan: 10/23/2010
OK
Cancel
Apply

Keep your computer protected

Your security software analyzes basic information about every file that you open, save, or download. For threats like viruses, it attempts to remove the threat from the infected file. If unable to remove the threat, it deletes the infected file along with the threat.

☑ Mark the **Scan for threats when opening, saving, or downloading files** checkbox to detect and eliminate security threats automatically.

Stay informed when something important happens

Important warnings appear when your security software deals with a threat.

☑ Mark the **Display a warning after detecting viruses, spyware, or suspicious behavior** checkbox to make sure you see these messages.

Schedule automatic scans

Some threats may remain hidden or dormant on the computer for a long time before they act. Your security software can find and stop such threats before they start to cause trouble.

Mark the **Conduct a scheduled scan of the computer** checkbox to check your files and settings for hidden threats.

Use the lists under the checkbox to select when the scan should begin. Choose a time when you would normally not use the computer very much after switching it on, like lunchtime on a Friday.

Maximize your protection

Your security software can not only search for threats in files and settings, but also check for suspicious behavior on your computer.

Mark the **Check if programs try to make unauthorized changes to system settings that could threaten your security** checkbox to block suspicious changes. Such changes can result in Web browser hijackings, unwanted but unremovable Web browser toolbars, or reduced computer performance, among other problems.

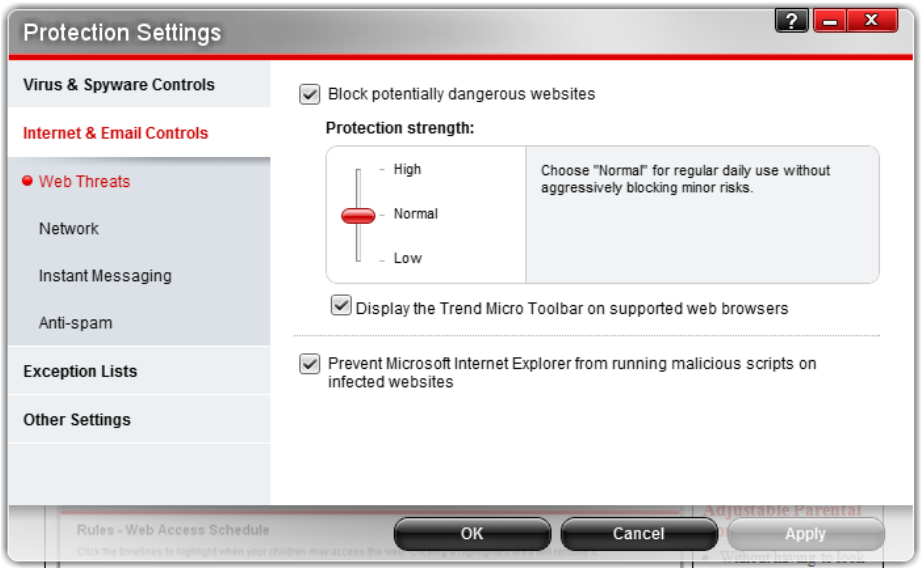
Mark the **Prevent programs on portable drives from launching automatically** checkbox to block programs that try to start running without your permission when you plug a USB drive into the computer. Flash memory or other portable USB drives rarely include certain kinds of programs that launch automatically, so they usually represent a threat if found.

If you have strong concerns about your security, then you can take even stronger measures against threats.

Mark the **Check compressed files, such as ZIP files, during real-time scans** checkbox to check files reduced in size through data compression techniques. Such files commonly end with the ZIP or RAR extension and require a specific program to "unpack," "unzip," or "decompress" the contents.

Mark the **Automatically delete files that show any signs of a threat** checkbox to get rid any file that might cause trouble. This aggressive response could remove some harmless files along with the unsafe ones, so consider using this protection only when receiving files or installing programs that seem risky.

20. Protection settings



Trend Micro maintains a database of risky websites that have a history of transmitting malicious software or supporting online fraud. Follow the directions below to protect yourself from unsafe sites.

Mark the **Block potentially dangerous websites** checkbox to protect against threats on the Internet automatically.

Choose one of the three levels of protection against Web threats:

High
Prevents you from opening sites that pose even a slight risk of transmitting viruses and spyware. This setting also blocks harmless sites that might have been hijacked in the past.

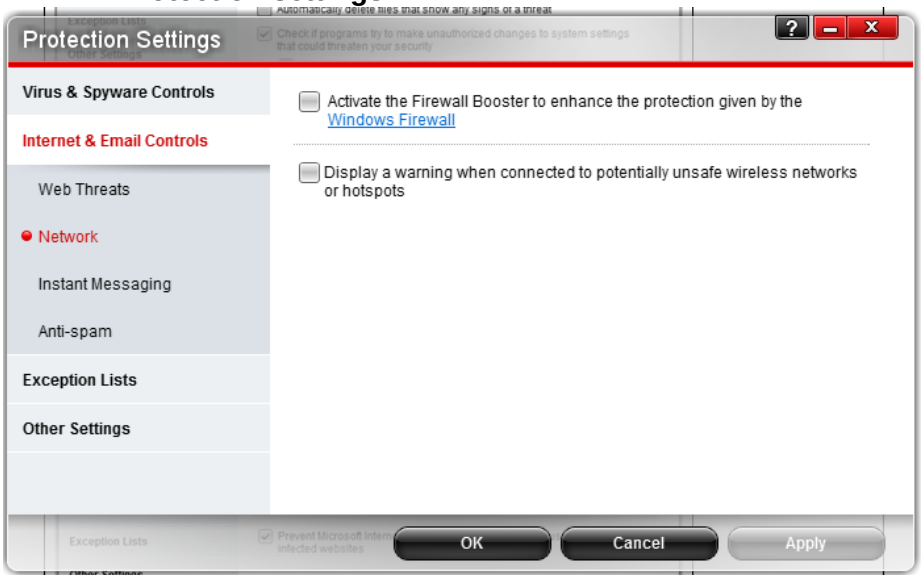
Normal
Blocks websites that have characteristics associated with online fraud, or that show signs of transmitting viruses and spyware. This setting also blocks unrated sites that might pose a threat.

Low
Only blocks websites verified as dangerous. These sites can transmit viruses and spyware or actively support online fraud.

Mark the **Display the Trend Micro Toolbar on supported web browsers** checkbox to make the Trend Micro Toolbar start checking for security risks in websites that you might want to open. The toolbar can also automatically rate the safety of links listed in online search results.

Mark the **Prevent Microsoft Internet Explorer from running malicious scripts on infected websites** checkbox to block dangerous software injected by hackers into legitimate websites.

21. Protection settings



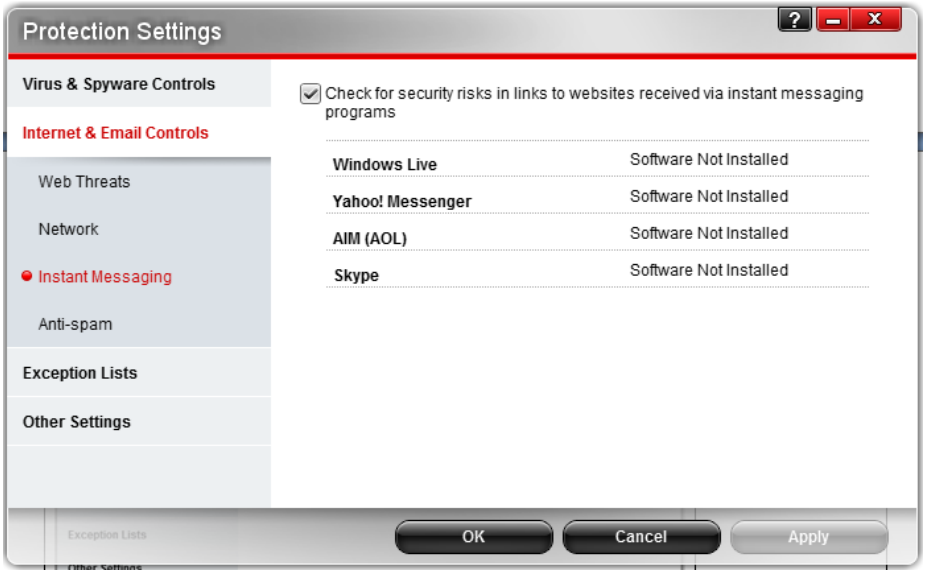
To help keep yourself safe on the Internet at home or on the go, you should mark both of these checkboxes.

☑ Mark the **Activate the Firewall Booster to enhance the protection given by the Windows Firewall** checkbox to configure the Windows Firewall so that it can offer better protection against online threats.

☑ Mark the **Display a warning when connected to potentially unsafe wireless networks or hotspots** checkbox to see a warning if you connect to a wireless network without trustworthy security credentials.

Only password-protected wireless networks are considered **safe**. Wireless networks that redirect your connection without encryption are considered **risky**. Wireless networks that do not have an authentication process or a valid security certificate rank as **dangerous**.

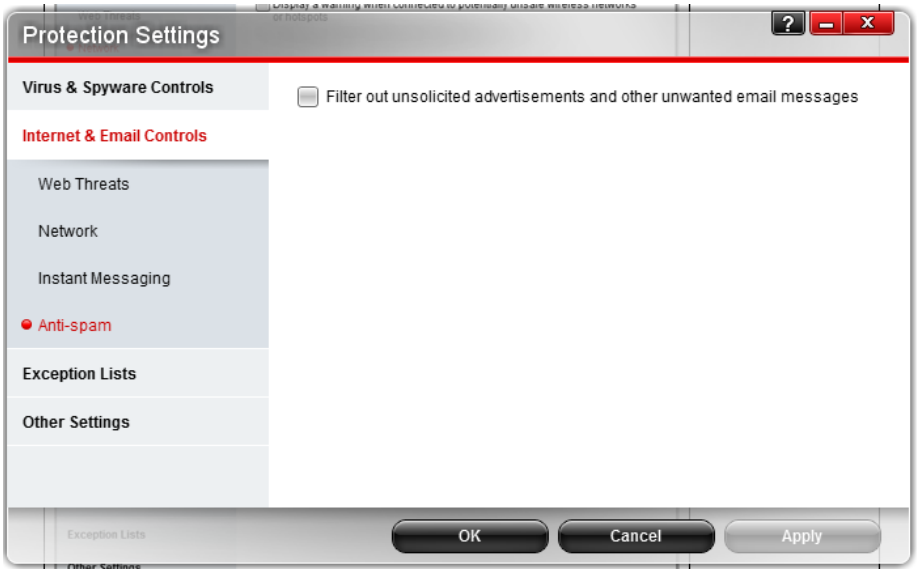
22. Protection settings



Your security software can protect you from links to unsafe websites sent via popular instant messaging programs.

☑ Mark the **Check for security risks in links to websites received via instant messaging programs** checkbox and then enable the protection for the instant messaging programs that you use.

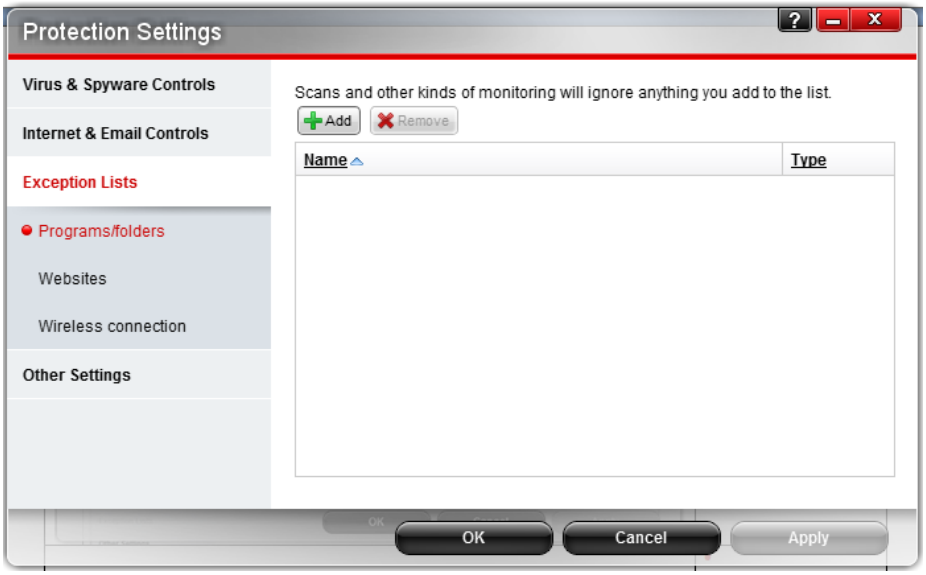
23. Protection settings



If you use email software on your computer, then you can use this feature to intercept unwanted email messages.

Mark the **Filter out unsolicited advertisements and other unwanted email messages** checkbox to activate the Trend Micro Anti-Spam toolbar in supported versions of Microsoft® Outlook®, Microsoft® Outlook® Express, and Windows Mail.

24. Protection settings



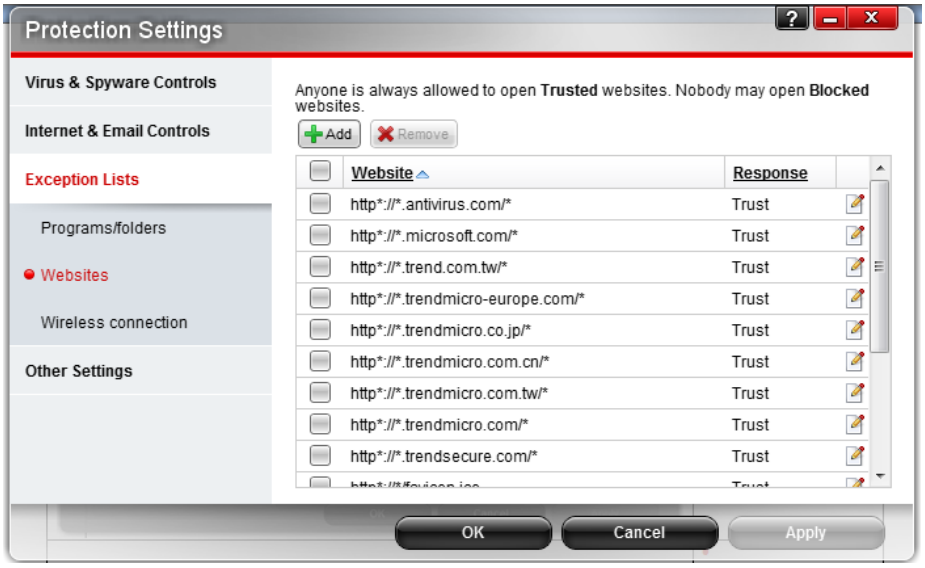
Programs/folders

You can use this exception list to speed up scans by making them ignore specific files or folders that you already consider safe.

25. Protection settings

- Click the **Add** button to open a window for selecting a file or folder to put on the list. You can only add one file or folder at a time.
- You can only use the **Remove** button after marking the checkbox next to at least one thing on the list.

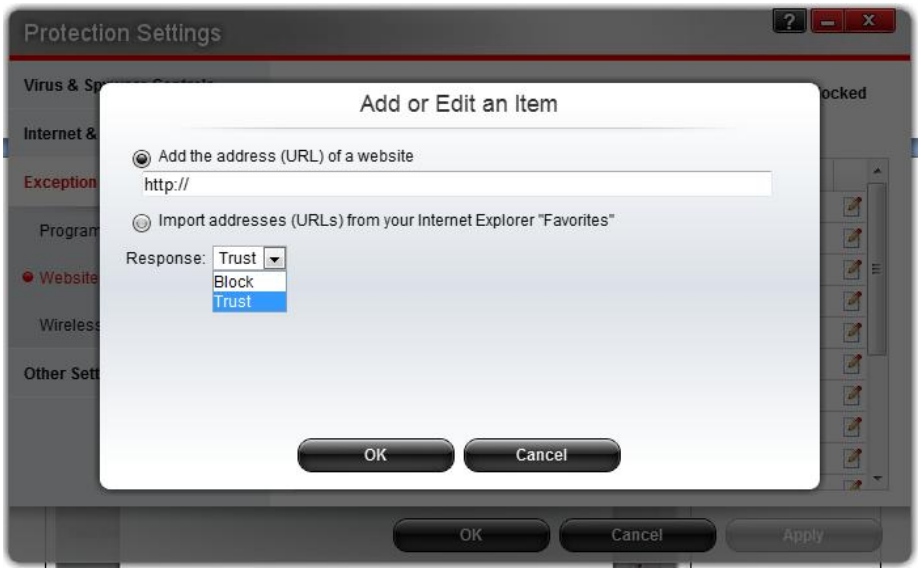
26. Protection settings



Websites

You can use this exception list to specify websites that should either always or never be blocked from opening.

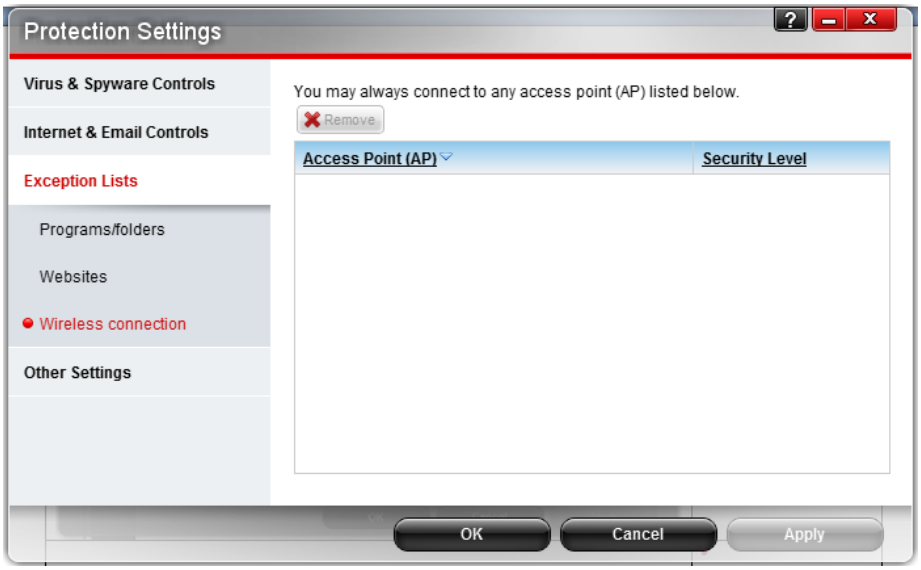
27. Protection settings



- Click the **Add** button to open a window for selecting a website to put on the list. After typing an address, select whether to **block** or **trust** that website from the dropdown list next to Response.

- You can click the **Remove** button after marking the checkbox next to at least one thing on the list.

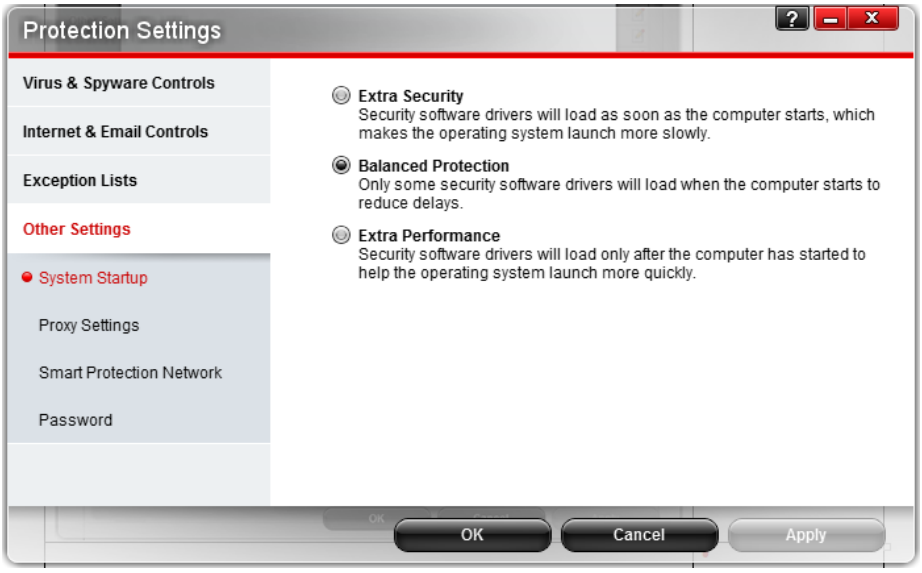
28. Protection settings



Wireless connection

Any wireless network identified as risky or dangerous that you have decided to trust will appear on this exception list. If you change your mind about trusting one of the networks, just mark the checkbox next to it and click the **Remove** button.

29. Protection settings


Protection Settings
Virus & Spyware Controls
Internet & Email Controls
Exception Lists
Other Settings
System Startup
Proxy Settings
Smart Protection Network
Password
Extra Security
Security software drivers will load as soon as the computer starts, which makes the operating system launch more slowly.
Balanced Protection
Only some security software drivers will load when the computer starts to reduce delays.
Extra Performance
Security software drivers will load only after the computer has started to help the operating system launch more quickly.
OK
Cancel
Apply

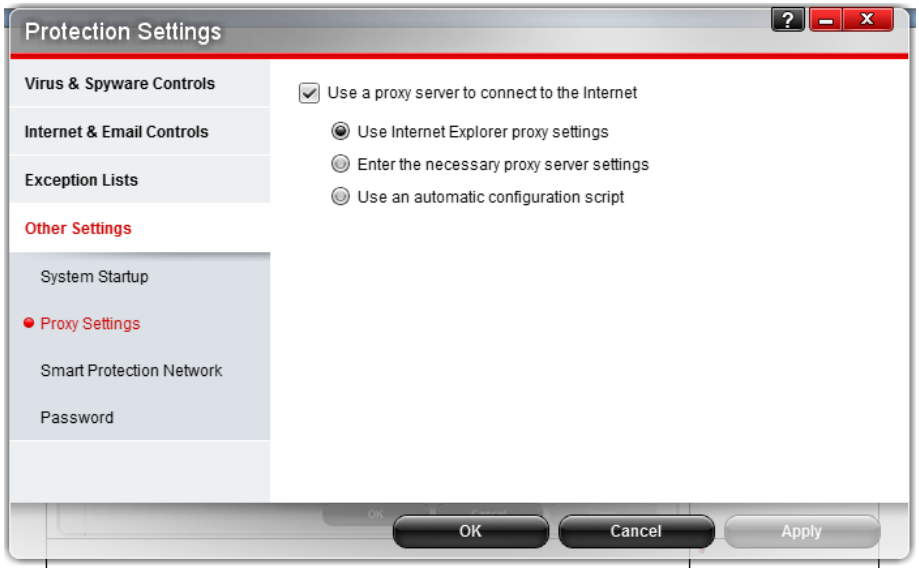
Your security software can load drivers and services gradually to help your computer start up as quickly as possible, or load them all immediately to provide the strongest security as soon as possible.

- Select **Extra Security** if you care most about protecting the computer as much as possible as soon as possible. You might have to wait a little bit longer for Microsoft Windows to launch when the computer starts.

- Choose **Extra Performance** if you prefer to avoid any delays caused by your security software when your computer starts. Most security software drivers will load only after Microsoft Windows has finished launching.

- If you do not know which option to choose, pick **Balanced Protection** to get the protection you need without sacrificing performance.

30. Protection settings



If your computer connects to the Internet through a proxy server, you can specify the proxy server settings on this screen.

Mark the **Use a proxy server to access the Internet** checkbox and configure the settings.

- **Use Internet Explorer proxy settings**

If you can successfully open websites with Internet Explorer (or do not know your proxy server settings), choose this option.

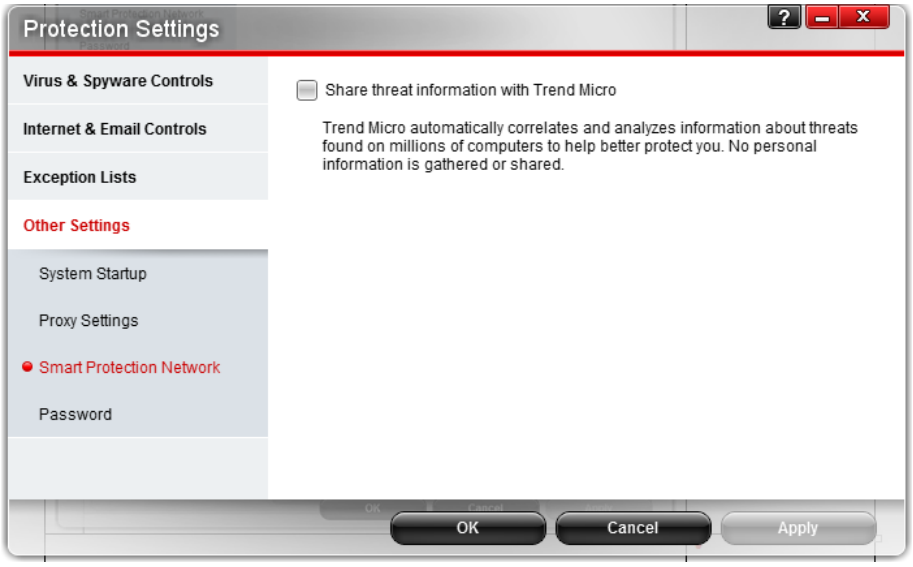
- **Enter the necessary proxy settings**

If you know your proxy server settings, choose this option and enter the required information.

- **Use an automatic configuration script**

If your proxy server uses a script or Proxy Auto-Configuration (PAC) file, paste the configuration script location or URL in the field (such as **http://FQDN/proxy.pac**).

31. Protection settings

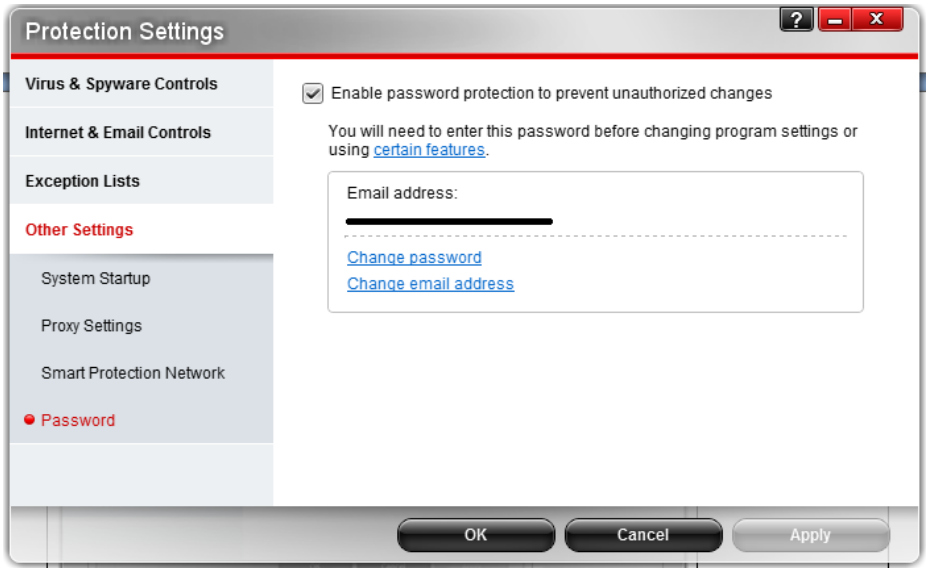

Protection Settings
Virus & Spyware Controls
Internet & Email Controls
Exception Lists
Other Settings
System Startup
Proxy Settings
Smart Protection Network
Password
Share threat information with Trend Micro
Trend Micro automatically correlates and analyzes information about threats found on millions of computers to help better protect you. No personal information is gathered or shared.
OK
Cancel
Apply

The Trend Micro Smart Protection Network™ automatically correlates information about security risks found on millions of computers worldwide to help develop protection against new threats more quickly. The more people participate, the more effective this network becomes.

Note: No personal information is gathered or shared.

☑ Mark the **Share threat information with Trend Micro** checkbox to help Trend Micro better protects you.

32. Protection settings

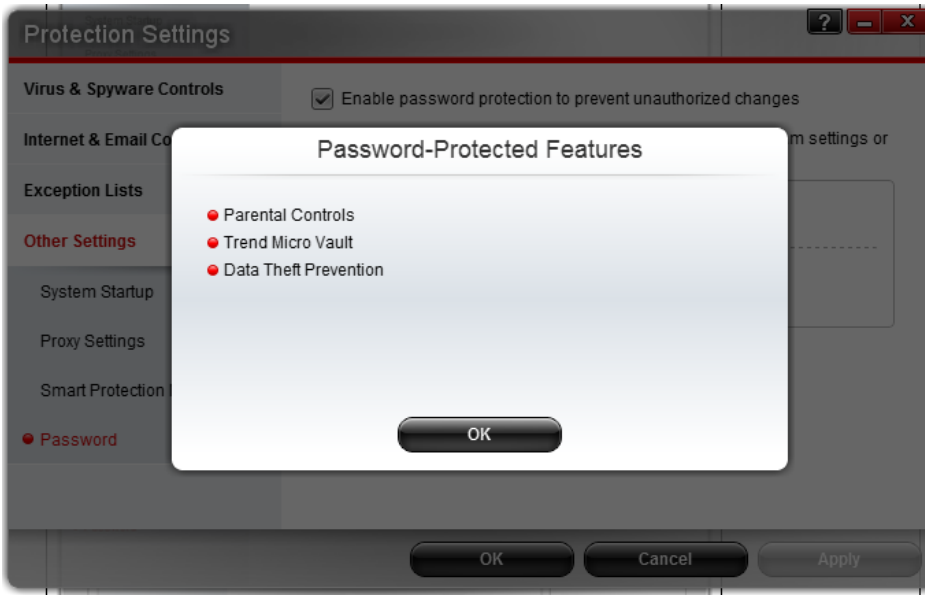


A password protects access to your security software and safeguards some of its features. Once you set a password, anyone who wants to shut down or uninstall the security software must provide the correct password.

Enable your password

1. On the main console, click the **Settings** button.
2. Under **Other Settings**, click **Password**.
3. Mark the **Enable password protection to prevent authorized changes** checkbox to set a password.
4. Provide an email address where you want the password sent if you forget it.
5. Type your case-sensitive password in the **Password** field.
6. Retype the same case-sensitive password in the **Confirm password** field.

33. Protection settings



Password required for access to:

- Parental Controls
- Trend Micro Vault
- Data Thief Prevention